UNITED STATES MARINE CORPS
MARINE AIR GROUND TASK FORCE TRAINING COMMAND
MARINE CORPS AIR GROUND COMBAT CENTER
BOX 788100
TWENTYNINE PALMS, CALIFORNIA 92278-8100

CCO 5230.1B
17/3
22 Aug 01

COMBAT CENTER ORDER 5230.1B

From: Commanding General
To: Distribution List

Subj: ELECTRONIC MAIL (E-MAIL) AND INTERNET USE ABOARD MCAGCC

Ref: (a) MCO 5271.4A
(b) ALMAR 068/97
(c) ALMAR 167/97
(d) ALMAR 162/00

1. Situation. To provide policy and guidance in accordance with the references regarding permissible and prohibited use of Electronic Mail (e-mail) and Internet for authorized users aboard the Marine Corps Air Ground Combat Center (MCAGCC) and for using Government information technology (IT) resources. Any violation of the prohibited activities listed below may result in administrative or disciplinary actions.

2. Cancellation. CCO 5230.1A.

3. Mission. To effectively regulate and control the access and use of Government IT resources through effective monitoring and timely corrective action to reduce and eliminate misuse of IT assets.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. To reduce and eliminate the unauthorized use of Government IT resources through effective monitoring and management.

(2) Concept of Operations. A Commanding Officer may use the logs and images as evidence in pursuing disciplinary action. Communication and Data Directorate (CDD) and the Center Inspector's office will be available for additional action as the Commanding Officer determines (e.g., disabling accounts, confiscating computers, initiating Naval Criminal Investigative Services (NCIS) oversight if child pornography, hate, or other extremist information has been identified).

b. Subordinate Element Missions

(1) Directors, Commanding Officers, and Officers-in-Charge

(a) Ensure that policy guidelines delineated herein are followed.

(b) Control and monitor internet access and usage within their respective units or organizations.

(2) Director, Communication and Data Directorate

(a) Monitor the proper use of e-mail and internet access, as well as network resources.

(b) Restrict access to e-mail and internet when required (i.e., misuse investigations, decreased network resources, etc.)

(c) Provide guidance and technical assistance on appropriate e-mail and internet access procedures and policies.

(d) Forward proxy logs of computers that have accessed inappropriate sites to the Center Inspector.

(3) Center Inspector

(a) Review proxy logs to determine the severity of computer network violation.

(b) Forward any proxy logs that contain material that could be considered criminal in nature, such as child pornography or hate sites to the NCIS for evaluation.

(c) Periodically submit articles to the Observation Post concerning computer usage.

(d) Disseminate all evidence to the appropriate unit Commanding Officer for appropriate disciplinary action.

(4) Individual Users

(a) Ensure that computer workstation is locked each time the user leaves his or her computer.

(b) Enable password protected screen saver on the computer terminal to ensure that the computer will default to a protected mode should the user walk away from the terminal without placing it in the locked mode.

(c) Protect the user password at all times by:

1 Allow no one to have access to user password.

2 When changing the password, utilize a password that is a minimum of 8 characters long, and is a combination of letters, (both upper and lower case) numbers, and symbols.

3 If a user password is compromised, immediately change the password by pressing the control key the alt key and the delete key at the same time as though logging in. Click the "change password" button and follow the steps for changing the user password.

(d) Ensure that computer workstation is logged off at the end of each day.

c. Coordinating Instructions

(1) Monitoring. The network will be monitored to ensure processing and network resources are not adversely impacted by internet use. Specific attention will be placed on internet applications, activities, and services that are bandwidth intensive and have a cumulative detrimental effect on telecommunications infrastructure.

(2) The procedures for monitoring internet usage will be as follows:

(a) CDD Security will check the daily proxy logs and print out the portions that identify an individual user or workstation accessing unauthorized sites.

(b) CDD Security will remotely access into the suspect computer and search the hard drive(s) for any inappropriate images, links, cookies, or files.

1 If inappropriate material is found, up to 5 images will be printed out.

2 The remote access will eliminate the need to confiscate any computers, or disable any e-mail accounts until directed by the unit Commander.

3 CDD Security will forward the logs and images to the Center Inspector's office for review.

4 The Inspector's office will disseminate all evidence to the appropriate agency for further investigation or to the appropriate unit Commanding Officer for disciplinary actions.

5. Administration and Logistics

a. Information

(1) Definitions

(a) E-mail is an authorized means of communication that uses computer-to-computer data transfer technology, normally in the form of textual messages. It also has the ability to carry a "payload" in the form of an attached file (i.e., text, graphics, programs, etc.).

(b) Organizational e-mail is any message or file transmitted to or from an authorized organizational mailbox. This is comparable to formal correspondence addressed generically to the commander or director of the organization. Reference (a) provides further guidance.

(c) An Organizational Mailbox (OMB) is the e-mail address of an office, activity, or command authorized to send or receive organizational e-mails. Only commands with a Plain Language Address (PLA) are authorized an OMB. The unit owning the mailbox will establish authorized users of this mailbox.

(d) Section e-mail is any message or file transmitted to or from a section's mailbox. Section e-mail can facilitate the exchange of information in the same way as the administrative distribution box.

(e) Section Mailbox (SMB) is the e-mail address of a subordinate office, activity or element of a command. Such offices are not authorized an organizational mailbox.

(f) Individual e-mail is a message or file transmitted to or from an individual's personal mailbox containing informal information that does not commit or direct an organization. The purpose of individual e-mail is to

facilitate the direct exchange of information in the same manner as the telephone, voice mail, or FAX machine.

(g) An Individual Mailbox (IMB) is the e-mail address of an individual. Per established security procedures, only the individual to whom it is assigned authorizes access to this mailbox.

(h) The internet is a global digital infrastructure that connects millions of computers and tens of millions of people.

(i) The World Wide Web (WWW) is a mechanism that simplifies the retrieval and display of information on the internet.

(j) The Non-secure Internet Protocol Router Network (NIPERNET) is a global digital infrastructure that provides a worldwide network for the DOD/DON/USMC and a path to the Internet.

(2) Guidelines

(a) E-mail

1 Per reference (a), e-mail is for official use only.

2 E-mail sent or received via the internet is authorized as long as:

a DOD maintains connectivity between the NIPERNET and the internet.

b It does not violate the criteria established in paragraph 5.c.(1) of this Order, for internet access.

(b) Each command authorized a PLA shall have an OMB.

(c) OMB/SMB/IMB naming conventions shall be per reference (a), and monitored by the CDD, Networking Branch.

b. Internet. There are two types of internet use: use of the internet through computers provided by private contractors or private organizations, and use on government computers. Use of the internet on computers provided by private contractors or private organizations for the use by Marines and Sailors and their family members will be governed by paragraph 5.a.(1) of this Order; use of the internet on government computers will be governed by paragraph 5.b.(2) of this Order. Due to current bandwidth limitations and network degradation, WWW broadcast media using "push technology" (i.e. Point-cast) is restricted.

(1) Prohibited use of the internet on computers provided by private contractors or private organizations include, but are not limited to, the following:

(a) Official work of a sensitive or classified nature.

(b) Illegal, fraudulent, or malicious activities.

(c) Chain letters.

(d) Unauthorized fundraising.

(e) Accessing, storing, processing, displaying or distributing offensive or obscene material such as pornography and hate literature.

(f) Obtaining, transporting, installing, or using software in violation of vendors' patent, copyright, trade secret or license agreement.

(g) Partisan political activity, political, or religious lobbying or advocacy of activities on behalf of organizations having no affiliation with the Marine Corps or DOD.

(2) All other uses of the internet on government computers will be per reference (d).

(a) Internet services may be used when work related and determined to be in the best interests of the Federal Government and the Marine Corps. Examples are:

1 Obtain information to support DOD/DON/USMC missions.

2 Obtain information that enhances the professional skills of military and civil service personnel.

3 Improve professional or personnel skills as part of a formal academic education or military and civilian professional development program (if approved by individual commands).

(b) Government computers may be used to access the internet for incidental personal purposes such as Internet searches and communications as long as such use:

1 Does not adversely affect the performance of duties.

2 Serves a legitimate professional interest such as enhancing personal skills or obtaining information.

3 Does not overburden Marine Corps computing resources or communication systems.

4 Not used for a purpose that adversely reflects upon the DOD/DON/USMC.

5 Is of minimal frequency and duration and occurs during an individual’s personal time.

6 Does not result in added costs to the government.

(c) Individual use of government resources to connect to the internet for purposes other than those described in the paragraphs above, is prohibited.

(d) Examples of prohibited internet use include, but are not limited to, the following:

1 Illegal, fraudulent, or malicious activities.

2 Partisan political activities, political, or religious lobbying or advocacy of activities on behalf of organizations having no affiliation with the DOD/DON/USMC.

3 Chain letters.

4 Unauthorized fundraising.

5 Accessing, storing, processing, displaying or distributing offensive or obscene material such as pornography and hate literature.

6 Obtaining, transporting, installing, or using software in violation of vendors' patent, copyright, trade secret or licensing agreements.

7 Storing, accessing, processing, or distributing classified, or otherwise sensitive information (e.g., privacy act, FOUO, proprietary, etc.).

c. Distribution. Distribution Statement A-1 directives issued by the Commanding General are distributed via guard mail. This Order can be viewed at http://www.29palms.usmc.mil/dirs/manpower/adj.

6. Command and Signal

a. Signal. This Order is effective date signed.

b. Command. This Order is applicable to the Marine Corps Total Force.

//signed//
JOSEPH F. WEBER

DISTRIBUTION: A-1